東 海 大 學 數 學 系 研 究 所

碩 士 論 文

指導教授：沈淵源

密封標單之研究

An Exploration On the Digital Sealed Bid

研究生：謝宏昌

中 華 民 國 九 十 九 年 六 月

東 海 大 學

數 學 系

碩士學位口試委員審定書

本系碩士班 謝宏昌 君

所提論文 On the Digital Sealed Bid
(密封標單之研究)

合於碩士班資格水準，業經本委員會評審通過，特此證明。

口試委員：

指導教授：

所 長：

中 華 民 國 九十九 年 六 月 十九 日

摘 要

近年來因為電腦和網路的發展，許多商業交易已經慢慢轉換到網路了。人們開始在網路上進行交易和買賣，因此交易的安全性和便利性，常常被人拿來研究。

本論文主要探討RSA密碼系統和橢圓曲線密碼系統使用在密封標單上之應用。首先論文分成三章，第一章前言介紹密碼系統在日常生活中的發展，進而發展至今日的電子商務如電子現金、電子競標上的應用。第二章介紹基本預備知識：RSA密碼系統和橢圓曲線密碼系統，以及雜湊函數和介紹電子競標的兩種分類：公開標單和密封標單。第三章是主要內容，將使用RSA密碼系統和橢圓曲線密碼系統應用在密封標單上，並比較兩種方法的不同。

誌 謝

本論文可以順利完成，在此必須感謝很多人，在東海大學研究所的這段期間，不論是學業或生活上，都接收到許多人的幫忙與協助。

首先要感謝我的指導教授沈淵源教授，一直給予我指導研究論文的方向，並不斷給予意見，讓我在撰寫論文過程中受益良多，最終才能完成此篇論文。在論文口試期間，曾琇瑱教授和陳淑珍教授的指導和指正，給予許多意見，讓這篇論文更加完整。此外在東海大學研究所這期間，感謝所有教授、助教、學長姐、全班同學，陪我走過這段日子，還有謝謝我的家人朋友給予支持。最後在此祝福大家，並分享我的喜悅。

目 錄

第一章　前言

人和人相處生活，溝通是生活中必備的生活方式。人不能離群獨居，獨自一個人自立更生，過著不與人交易的生活。即使是動物也會有其溝通方式，人和人交流就會產生交換訊息的方式：如說話、寫字等等。通訊即是生活中每日要做的事。人類總是生性多疑，深怕自己傳送給人的訊息被第三人知道，害怕被第三人給攔截或修改。因此，就希望能以一種方式除收訊人之外，沒人可以解讀的方式來傳送訊息。因為有了保護彼此秘密通訊的慾望，這種傳訊方式，慢慢沿生為密碼學的開端。

隨著網際網路的發達，大量的文字、圖片、或影音等數位資訊在電腦網路上不斷地傳遞交換。此時因為科技的便利，也提升傳遞資訊的速度，但同時也需要顧慮到其安全性。因此密碼學技術逐漸被引用到網際網路的世界了。是故也因此產生了許多新的密碼技術：如 RSA、EIGamal、橢圓曲線密碼系統等等，都是被應用至電腦網際網路的傳訊加密技術、數位簽章等等。電子商務如電子付款、電子現金、電子支票、電子交易、至本論文所探討的電子競標，是近年來商業流通在網際網路的新概念。漸漸的電子商業會慢慢取代傳統市場，會變成一種線上買賣的趨勢，因此涉及金錢交易的行為，保障電子商務的安全性變成一種大家所追求研究的方向。本篇論文由探討 RSA 密碼系統和橢圓曲線密碼系統和電子競標上的應用；最後研究其兩者方式在電子競標秘密投標的應用。

第二章　預備知識

2.1 RSA 密碼系統

2.1.1 RSA 簡介

1976 年左右，史丹佛大學學生 Whitfield Diffie 和他的教授 Martin Hellman 開始研究有關鑰匙交換的問題，便揭開了現今非對稱鑰匙密碼學的構想。基於非對稱鑰匙密碼學，Whitfield Diffie 和 Martin Hellman 的構想，1978 年，由美國麻省理工學院的三位教授 Rivest、Shamir 及 Adleman 發展出第一個公開鑰匙密碼系統，即所謂的 RSA 密碼系統。至今 RSA 依然是被廣泛使用的公開鑰匙機制。他解決鑰匙協定和分配問題，使用了新概念，利用公開鑰匙(pubic key)和私密鑰匙(private key)來使密碼學更進一大步。

2.1.2 RSA 演算法

一. 鑰匙生成方式

(1)每位使用者，選擇兩個大質數 p 和 q

(2)計算　$n = pq$

(3)計算　$\phi(n) = (p-1)(q-1)$

(4)選擇公開鑰匙 $e \in Z^+$ 且 $\gcd(e,\phi(n))=1$ ， $1<e<\phi(n)$

(5)製造私密鑰匙 $d \equiv e^{-1} \pmod{\phi(n)}$

(6)產生 public key $\alpha=\{n,e\}$

(7)產生 private key $\beta=\{n,d\}$

二. 加密演算 (Encryption)

(1) 明文(plaintext) $M < n$

(2) 密文(ciphertext) $C \equiv M^e \pmod{n}$

三. 解密演算 (Decryption)

(1) 密文(ciphertext) C

(2) 明文(plaintext) $M \equiv C^d \pmod{n}$

例題：

1. 令 $p=47$ 和 $q=71$

2. 計算 $n=pq=47\times71=3337$

3. 計算 $\phi(n)=(p-1)(q-1)=46\times70=3220$

4. 選擇公開鑰匙 $e \in Z^+$ 且 $\gcd(e,3220)=1$ ， $1<e<3220$ ，

$3220=2\times2\times5\times7\times23$ 須選擇不含因數 2, 5, 7, 23 的數

，故選 $e=79$

5. 私密鑰匙 $d \equiv e^{-1} \pmod{3220}$

$79d \equiv 1 \pmod{3220} \Rightarrow 80501 = 1019 \times 79 \equiv 1 \pmod{3220}$

public key $\alpha = \{3337, 79\}$

private key $\beta = \{3337, 1019\}$

二. 加密演算 (Encryption)

密文(ciphertext) $C \equiv M^e \pmod{n}$

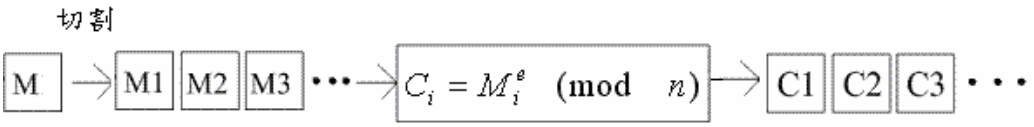
$IF \quad M = 668$ ， $C \equiv 668^{79} \pmod{3337}$
$\equiv 1570 \pmod{3337}$

三. 解密演算 (Decryption)

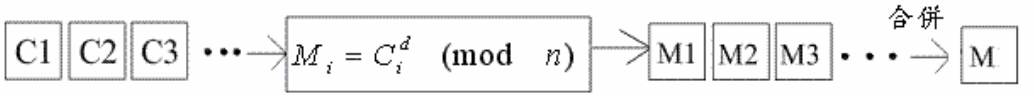
明文(plaintext) $M \equiv C^d \pmod{n}$
$\equiv 1570^{1019} \pmod{3337}$
$\equiv 668$

RSA 加解密流程圖：

加密流程圖：



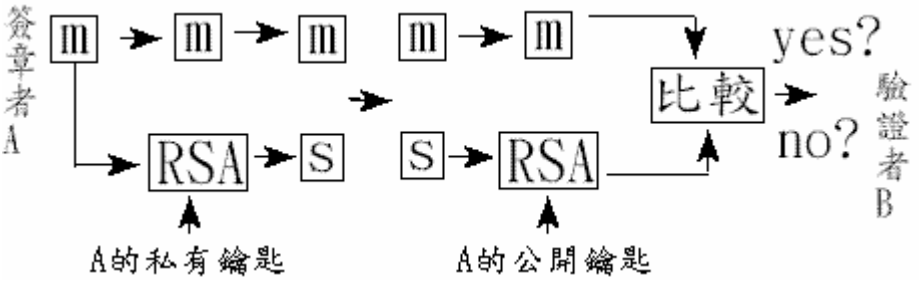
解密流程圖：



2.1.3 RSA 數位簽章

隨著公開鑰匙密碼學的發展，數位簽章(Digital Signature) 是最重要的果實。數位簽章和一般簽章流程是一樣的，只是一般簽章是用印章，而數位簽章是用”密碼學這把鑰匙”。

RSA 數位簽章流程圖：



設簽章者 A 欲將文件 m 作數位簽章，必須使用私有秘密鑰匙 d_A，然後對 m 加以簽署獲得簽署文 s。

簽署： $s \equiv m^{d_A} \pmod{n_A}$

並將 m 及簽署文 s 傳送至驗證者 B，驗證者 B 使用簽章者 A 之公開鑰匙 e_A 進行驗證。

驗證： $m' \equiv s^{e_A} \pmod{n_A}$

若 $m' = m$ 即驗證正確，否則失效。

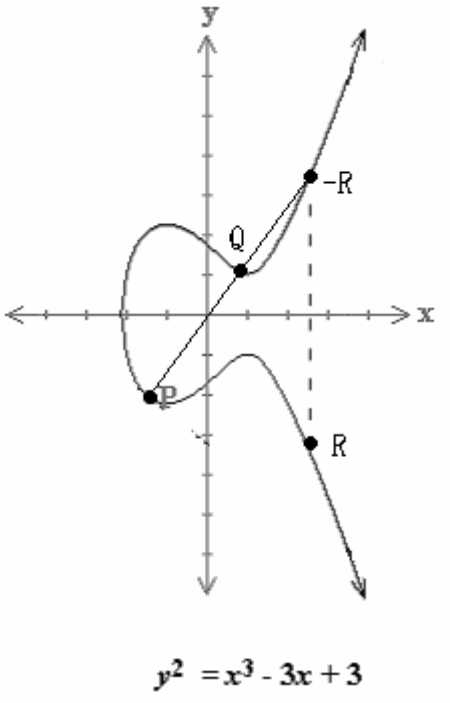
2.2 橢圓曲線密碼系統

2.2.1 發展簡介

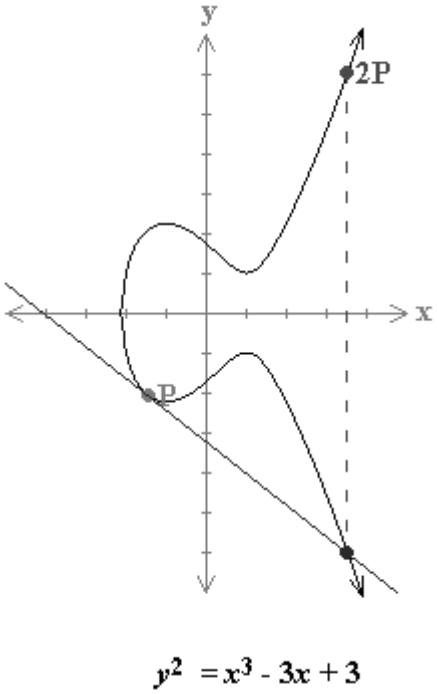
1920 年代中期，米勒(Miller)和寇伯茲(Koblitz)將橢圓曲線引進至密碼學中，而藍斯特拉(Lenstra)則指出如何使用橢圓曲線來分解因數。是故，在加解密碼系統上比較，橢圓曲線產生的鑰匙，其所佔用的位元遠比相同安全度上的其他非對稱公開鑰匙來說更為精簡。因此運算速度也增快許多。所以近代很多密碼學都漸漸應用在橢圓曲線上了。

2.2.2 橢圓曲線加法規則

橢圓曲線方程式，表示為 $y^2 = x^3 + ax + b \pmod{p}$，其中 $a, b \in Z_p$，任何一曲橢圓曲限定義中會有一個元素稱之為無線點(point at infinity)或零點(zero point)以符號 ∞ 表示之。



圖(1)兩個相異點相加



圖(2)雙倍的 P 點

(1) 在橢圓曲線 E 上給相異兩點相加 P 和 Q 相加可得到第三點 R，P+Q=R，其作圖方式：經過 P 和 Q 兩點作一直線 L 與橢圓曲線 E 相交與(-R)點。再橢圓曲線上取一點與(-R)點相對稱於 X 軸之點，即是 R 點。如圖(1)。

(2) 在橢圓取線 E 上取一點，承(1)若 P=Q 時，P+Q=P+P=2P=R，其作圖方式：對 P 點作一切線 L，L 與橢圓取線 E 相交於一點，接著對 S 點作對稱於 X 軸的點，即是 2P 點。如圖(2)

(3) 加法單位元 ∞，即橢圓取線上任一點

$p = (x, y) \Rightarrow p + \infty = \infty + p = p$，且 $p + (-p) = \infty$，

故 $-p = (x, -y)$，稱為 p 加法反元素。

(4) 結合性 $(P+Q)+R=P+(Q+R)$，

交換性 $Q+P=P+Q$

(5) 橢圓曲線加法運算公式，令 E 為橢圓曲線 $y^2=x^3+ax+b$，令 $P=(x_1,y_1)$，$Q=(x_2,y_2)$ 為 E 上之兩點，則 $P+Q=R=(x_3,y_3)$

可得 $x_3=m^2-x_1-x_2$

$$y_3=-[m(x_3-x_1)+y_1]$$

其中 m 為，$m=\begin{cases}\dfrac{(y_2-y_1)}{(x_2-x_1)} & 若P\neq Q\\ \dfrac{(3x_1^2+a)}{2y_1} & 若P=Q\end{cases}$

2.2.3 橢圓曲線加解密碼系統

橢圓曲線加解密方法有許多種，近年來發展快速，如 Koblitz 與 Menezes-Vanstone 橢圓曲線密碼系統等等，因為橢圓曲線是一種很新穎的東西，大多應用在大數分解質數判斷、加解密、數位簽署、鑰匙交換等等，以下介紹其中一種橢圓曲線加解密的方法。

橢圓曲線的公開鑰匙加解密機制：

使用者 A 將明文加密傳給使用者 B：

(1) 公開橢圓曲線 $E_p(a,b)$：$y^2 = x^3 + ax + b \pmod{p}$，

在橢圓曲線 $E_p(a,b)$ 上取任一點 G，G 是公開點。

使用者 B 的公開鑰匙 $B = KG$（設使用者 B 私密鑰匙 K）。

假設明文為 M，設 $M = M_1 + M_2$

(2) 選擇一亂數 r，並計算 $R = rG$。

(3) 計算 $C_1 = M_1 + (rB)_x$，C_1, M_1 為一個數值，(rB) 為座標，

故取 x 座標值計算相加。

計算 $C_2 = M_2 + (rB)_y$，C_2, M_2 為一個數值，(rB) 為座標，

故取 y 座標值計算相加。

(4) 傳送 C_1, C_2, R 給使用者 B。

(5) 使用者 B，利用 C_1, C_2, R

計算 $M_1 = C_1 - (KR)_x$

$M_2 = C_2 - (KR)_y$ ，得到 $M_1 + M_2 = M$

補充

$$
\begin{aligned}
&M_1 \\
&= C_1 - (KR)_x \\
&= M_1 + (rB)_x - (KrG)_x (\because R_x = (rG)_X) \\
&= M_1 + (rB)_x - (rB)_x (\because B_x = (KG)_x) \\
&= M_1
\end{aligned}
$$

2.2.4 橢圓曲線的數位簽章

使用者 A 做數位簽章傳給使用者 B：

(1) 公開橢圓曲線 $E_p(a,b)$ ： $y^2 = x^3 + ax + b \pmod{p}$ ，

在橢圓曲線 E 上取任一點 G ， G 是公開點。

使用者 A 私密鑰匙 K ，使用者 A 的公開鑰匙 $B = KG$ 。

假設要簽署的訊息為 M 。

(2) 選擇一亂數 r ，並計算 $R = rG$ 。

(3) 計算 $S = r^{-1}(M - KR_x)$ ， r^{-1} 為 r 的反元素， R_x 為 R 的 x 座標值。

(4) 傳送 M, S, R 給使用者 B， S , R 作為簽署文。

(5) 使用者 B，利用 M, S, R

驗證方法： $V_1 = R_x B + SR$

$V_2 = MG$ ， 檢驗 $V_1 \stackrel{?}{=} V_2$

2.3　雜湊函數(Hash function)

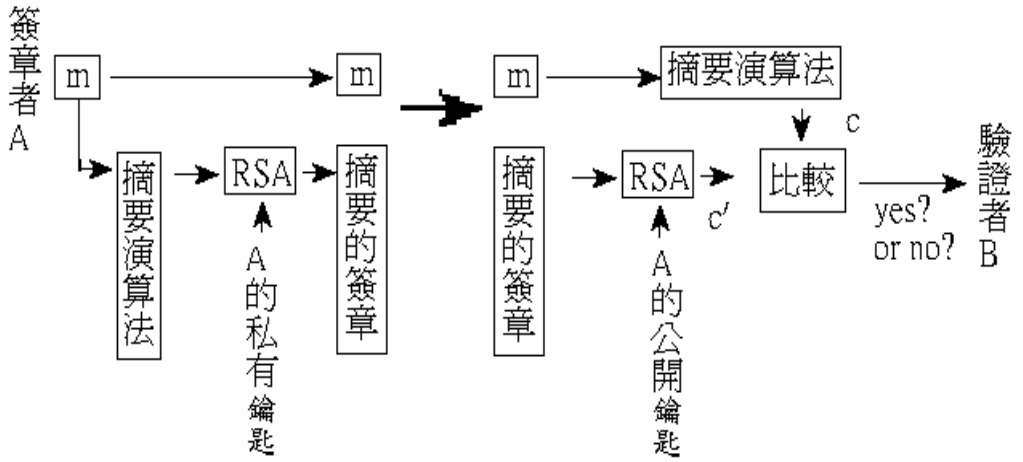
因為RSA演算法速度太慢於是數學家想出減少明文長度的方法，因此有了訊息摘要的概念。在密碼學領域中，把”訊息摘要演算法”亦稱為”雜湊函數”。Hash function是一種單向函數(one-way function)：

(1)　給一個函數 f 對於任意的輸入值 x，可以得到 $y = f(x)$。

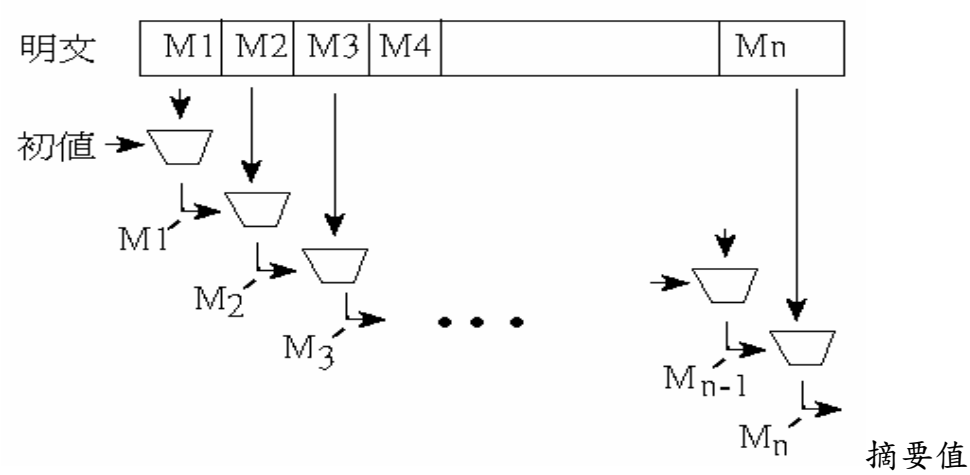
(2)　函數 $y = f(x)$ 中任一個 y，求解 $x = f^{-1}(y)$ 是計算不出來的。

Hash function是任一長度的訊息輸入可成為一個長度較短且固定輸出的運算，即為訊息摘要 (Digest)。

利用明文摘要的簽章流程圖：



摘要演算法流程圖：



(1) 先把明文拆成M_1、M_2、、、M_n固定長度，其中M_n以特定方式將其補至固定長度。

(2) 梯形面積是一種演算方式，梯形面積內的運算都是一些基本運算(如加法、位移等等)，因此 Hash function 運算速度很快。

(3) 首先M_1和初值經演算法，得到M_1'再和M_2演算如此下去，直至M_n'被求出，即是明文訊息摘要(hash value)。

(4) 常用的 Hash function 演算法如 MD5 等等。MD5(Message Digest Algorithm Version5)，MD5 主要來驗證所傳訊息的確認性。

2.4　電子競標

2.4.1　電子競標簡介

隨著電腦網路的進步發達，傳統的市場拍賣形式，以另一種方式出現在網際網路上，即電子競標系統和網路拍賣，電子競標在現今商業交易日益增多，如 YAHOO!拍賣、eBay 拍賣網等等。

目前電子競標主要有三種形式：

(1)　英式拍賣：最常見的一種拍賣方式。首先由主持拍賣會的主持人負責整個競標過程的流程及秩序。競標者在拍賣會場，當場出價競標，競標品由一個底價開始向上喊價，競標者必須喊比上一個競標者還要高的價錢，直至沒有其他競標者高過此價錢，即以此價錢得標。此類型競標方式，常見於中古市場、古董拍賣會等等地方。

(2)　最高價秘密競標(First-price Sealed-bid Auction)：競標者將所想要競標的價錢，寫在競標單或競標書上，以信封方式密封，於截止日前，交到拍賣者手上，賣家於開標日，將信封打開，以競標單上的價錢進行比較，以出價最高者的得標。此種競標方式常用於工程投標等等。

(3)　第二高價秘密競標(Second-price Sealed-bid Auction)：

競標者將所想要競標的價錢，寫在競標單或競標書上，以信封方式密封，於截止日前，交到拍賣者手上，賣家於開標日，將信封打開，以競標單上的價錢進行比較，以出價第二最高者的得標。

2.4.2　電子競標應具有的特性

電子競標過程中要保護競標者的匿名性及投標資訊，任何人都無法獲得競標者的身份和投標訊息內容。競標結束只公開得標者的身分和最高價，任何人皆可以驗證其結果的有效性。

大略介紹一些特性如下：

一.　競標者的匿名性：即使在拍賣結束，任何人都無法得知競標失敗者的身分及其所出的價錢。

二.　不可抵賴性：得標者不可否認其所出的價錢。

三.　公開驗證性：任何人皆可以驗證得標者的有效性。

四.　不可欺騙性：不能偽裝已註冊者的身分進行競價。

五.　協議健狀性：即使投標中有人無效，拍賣過程依然正常運作。

2.4.3 電子競標系統流程

C.C. Chang and Y.F. Chang 在 2003 年提出一種實用的電子競標系統，加速網路拍賣的發展，也奠定一定的電子競標系統的架構。

電子競標系統推演：

系統中必須存在一個憑證機構(Certificate Authority , CA)，這是電子競標系統中代表公平公正的第三方，CA 主要的功能：發給個人憑證和公開個人鑰匙。其中拍賣者以 B 表示，投標者以 A 表示。每一個投標者 A 有一把公開鑰匙α_A和一把私密鑰匙β_A，拍賣者 B 也有一把公開鑰匙α_B和私密鑰匙β_B，CA 會發給每一個投標人和拍賣者一個個人憑證。接著拍賣者和投標者會協調出一把共享鑰匙α_T，或由 CA 提供。

投標前拍賣者 B 會和投標者 A 用共享鑰匙α_T來驗證彼此身分。投標者 B 會選擇一個數M並計算$R = h(M,T,\alpha_T)$，並將(M,T,α_T)傳給拍賣者 A，其中h函數是 Hash function，T是表示下標時間。拍賣者 B 收到(M,T,α_T)，即算出$R' = h(M,T,\alpha_T)$，若$R = R'$即驗證通過，即簽章核可。拍賣者 B 算出$G = h((M+1),\alpha_T)$並廣播出去，即代表競標者身分確認無誤。

競標過程：

（1）$S = E_{\beta_A}(B \| T)$，投標者 A 用私密鑰匙β_A將自己出價B和競標時間T做加密得到S。

(2) $D = E_{\alpha_B}(S)$，投標者 A 使用 B 公開鑰匙來加密得到 D。

(3) 使用者 A 算出 $C = h(B,T,\alpha_T)$ 並將 (B,T,D,C) 送出。

$$C' = h(B,T,\alpha_T)$$

$$S' = D_{\beta_B}(E_{\alpha_B}(S))$$

(4) 若 $C' = C$，驗證 $B \| T \stackrel{?}{=} D_{\alpha_A}(E_{\beta_A}(B' \| T'))$ 是否成立，

成立就表示此標示合法的，否則拍賣者 B 會公告這個標是不合法的。

(5)若 $C' \neq C$，公告這個標 (B,T,D,C) 是不合法的。

2.4.4 電子競標的兩種系統

(1)公開標單 (Public Bid)：

投標價錢需一直向上攀升，直至沒有投標者願意出更佳的投標價為止，又稱為多次投標型的競標方式 (Multi-Bidding Auction)。

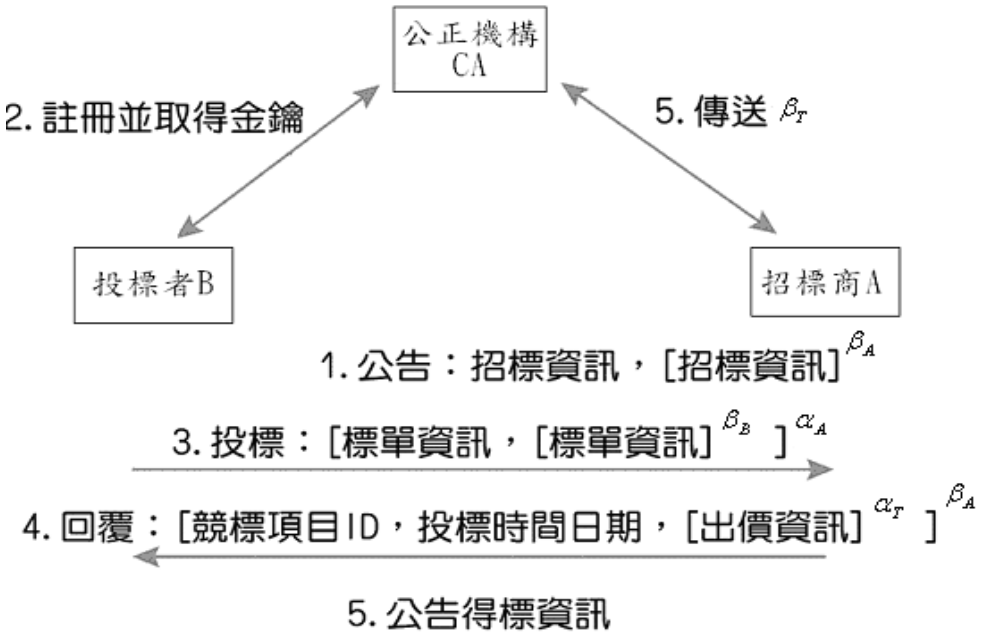
(2)密封標單 (Sealed Bid)：

投標者將金額放入密封標單，直到投標時間終止拍賣者進行開標作業，又稱單次投標方式 (Single-Bidding Auction)。

第三章　密封投標的研究

本論文探討將使用 RSA 系統和 RSA 數位簽署，與橢圓曲線密碼系統及橢圓曲線數位簽署在密封投標的研究並比較，故特別介紹電子競標中秘密競標系統的流程。

密封標單電子競標流程圖：



招標資訊=[競標項目、競標項目的 ID、開標時間日期、專屬此競標項目之公開鑰匙α_T、及參與之公正單位。]

標單資訊=[競標項目 ID、公開鑰匙α_B、核發鑰匙之機構、投標時間日期、[*出價資訊*]$^{\alpha_T}$]。

拍賣商 A (Auction)一組公開鑰匙α_A和私密鑰匙β_A

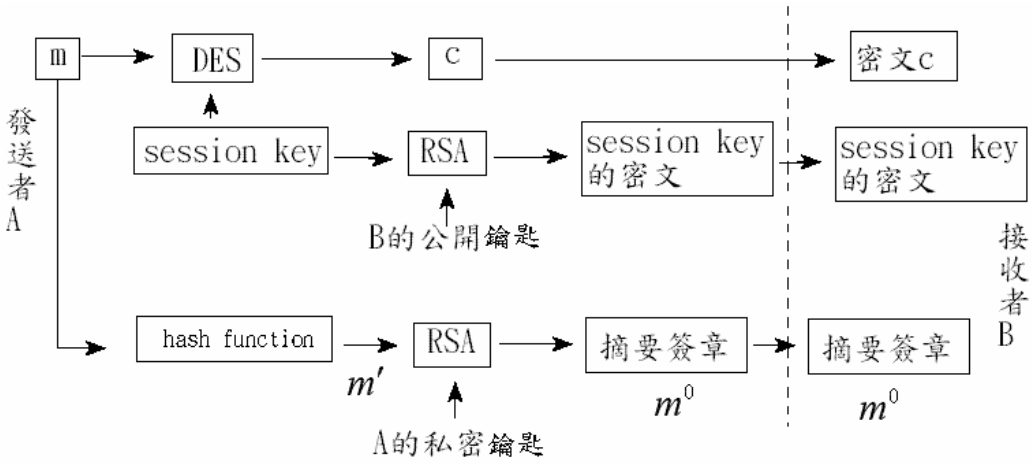
投標者 B (Bidding)一組公開鑰匙α_B和私密鑰匙β_B

公正機構(CA) 一組公開鑰匙α_T和私密鑰匙β_T

3.1 使用 RSA 在密封投標上

整合對稱非對稱密碼系統、訊息摘要及數位簽章系統，根據 RSA 非對稱密碼系統，主要運算來自繁雜指數運算，是否可利用對稱式密碼系統如 DES 對稱式密碼系統和訊息摘要演算法來加快運算速度。

加密流程圖如下：



步驟(1)：發送者 A 將明文m，輸入 DES 演算法，得到密文c。

步驟(2)：發送者 A 自行隨機取出一組 56 位元長的亂數當 DES 加密鑰匙，也當做 DES 加密演算法的輸入，此演算法的輸入此亂數值為 session key，即此次通訊中使用的交談鑰匙(session key)。

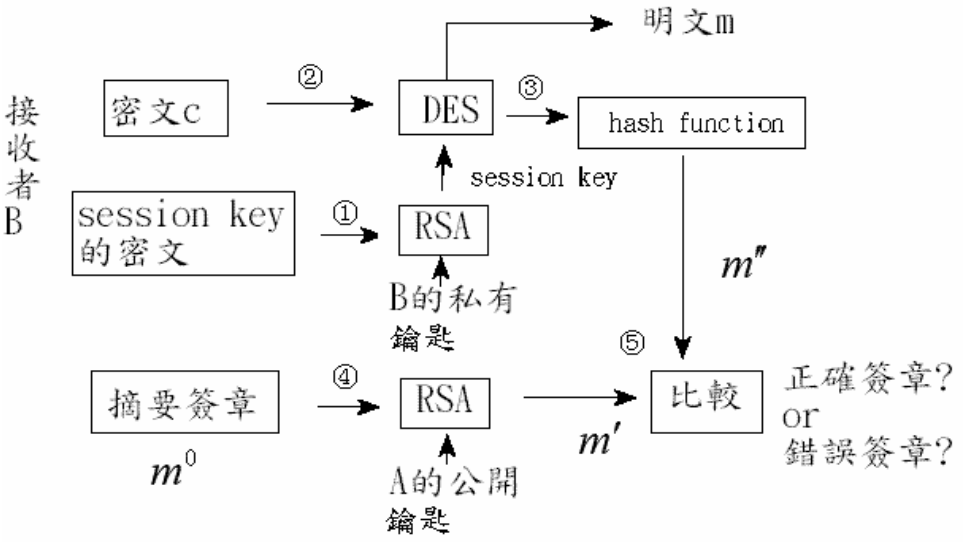
步驟(3)：由於交談鑰匙(session key)由發送者 A 所隨機產生需傳送給接收者 B 使用來解密。故發送者 A 利用 RSA 密碼系統將交談鑰匙加密傳至接收者 B。

步驟(4)：將明文經訊息摘要演算法(hash function 如 MD5)得到一個”訊息摘要值m'”。

步驟(5)：“訊息摘要值m'”可以代表明文本身，將其代入 RSA 簽章演算，生成一個”訊息摘要的簽章m^0”。

步驟(6)：將密文c，session key 的密文，和訊息摘要的簽章m^0，一並送到接收者 B。

解密流程圖：



步驟(1)：接收者 B 無法直接對密文 c 解密，須先將 session key 的密文解開，得到 session key。

步驟(2)：session key 是加解密文 c 的 key，因此將密文及 session key 輸入 DES 演算中，即解密成功得到明文。

步驟(3)：將明文 m 輸入訊息摘要演算法(hash function 如 MD5)，產生一個訊息摘要 m''。

步驟(4)：將訊息摘要 m^0，以 RSA 演算法解密，得到訊息摘要 m'。

步驟(5)：比較 m' 和 m'' 是否簽章正確。

使用 RSA 流程在密封投標

首由 CA 公正機構，發給招標商 A 一組公開鑰匙 α_A 和私密鑰匙 β_A，和一個 CA 認證的公開鑰匙 α_T，首先招標商 A 廣播”招標資訊”(競標項目 ID、開標時間 T、專屬此競標項目之公開鑰匙 α_T)。

步驟(1)：招標商 A 將招標訊息(如：m)，輸入(hash function 如 MD5)得到一個”招標訊息摘要值(如：m')”，招標訊息摘要值(如：m')再輸入 RSA 數位簽章系統，由 β_A 進行加密，得到”招標訊息摘要的簽章(如：s)”，將(招標訊息,招標訊息摘要值簽章)(如：m, s)公佈出去。

例:

設 hash function 為 $f(x) \equiv x(\text{mod } k)$ ，即 x 除以某個數值 k ，取其餘數為 $f(x)$ 。 k 是除數, 求出的餘數介於 0 至 $k-1$ 之間。

首先公正機構 CA： $n_T = p_T \times q_T = 109 \times 229 = 24961$

$$\phi(n_T) = (p_T - 1) \times (q_T - 1) = 108 \times 228 = 24624$$

取公開鑰匙 $\alpha_T = (24961, 125)$

私密鑰匙 $\beta_T = (24961, 197)$

設招標訊息 M_A=(ID, time, α_T)=(219 ,0611 ,125)

$x = M_A$ ，取 $k = 100$ ， $m_A = f(x) = (m'_A, m''_A, m'''_A) = (19, 11, 25)$

設 $p_A = 101$ ， $q_A = 211$

$n_A = p_A \times q_A = 101 \times 211 = 21311$ ， $(p_A - 1)(q_A - 1) = 21000$

取 $e_A = 97$ ， $e_A d_A \equiv 1 \pmod{21311} \Rightarrow d_A = 433$

公開鑰匙 $\alpha_A = (n_A, e_A) = (21311, 97)$

私密鑰匙 $\beta_A = (n_A, d_A) = (21311, 433)$

簽章 $s_A \equiv m_A{}^{\beta_A} \pmod{n_A}$ ，

$$s'_A \equiv 19^{433} \pmod{21311} \equiv 4092 \pmod{21311}$$

$$s''_A \equiv 11^{433} \pmod{21311} \equiv 16522 \pmod{21311}$$

$$s'''_A \equiv 25^{433} \pmod{21311} \equiv 11545 \pmod{21311}$$

公告 (M_A, s_A) ， M_A = (219 ,0611 ,125)

$$s_A = (s'_A, s''_A, s'''_A) = (4092, 16522, 11545)$$

步驟(2):投標者 B 向 CA 註冊並獲得一組鑰匙,公開鑰匙α_B和私密鑰匙β_B。

例:

設 $p_B = 103$ ， $q_B = 223$

$n_B = p_B \times q_B = 103 \times 223 = 22969$

$(p_B - 1) \times (q_B - 1) = 102 \times 222 = 22644$

取 $e_B = 53$ ， $e_B d_B \equiv 1 \pmod{22644} \Rightarrow d_B = 1709$

公開鑰匙 $\alpha_B = (n_B, e_B) = (22969, 53)$

私密鑰匙 $\beta_B = (n_B, d_B) = (22969, 1709)$

步驟(3)： 假設”標單資訊”=[競標項目 ID、α_B、投標時間 T、

[*出價資訊*]$^{\alpha_T}$]。

（首先將”出價資訊”做 RSA 加密使用公開鑰匙α_T，

得到[*出價資訊*]$^{\alpha_T}$ ）。

投標者 B 將”標單資訊“(如：m_0) 輸入(hash function 如 MD5)

得到一個”標單資訊摘要值(如：m_0')”。標單資訊摘要值(如：m_0')

再輸入 RSA 數位簽章系統，由β_B進行加密，得到”標單資訊摘

要的簽章(如：s')” 。

將(標單資訊, 標單資訊摘要值簽章)(如：m_0, s')，

再以α_A公開鑰匙以 RSA 法加密，

得到$\left(\text{標單資訊,標單資訊摘要值}^{\beta_B}\right)^{\alpha_A}$，傳送給招標商 A。

招標商 A 將$\left(\text{標單資訊,標單資訊摘要值}^{\beta_B}\right)^{\alpha_A}$

，以私密鑰匙β_A解密，得到(標單資訊, 標單資訊摘要值簽

章)($\left(\text{標單資訊 ,標單資訊摘要 值}^{\beta_B}\right)$(如：$m_0$, s'))。

將”標單資訊摘要值簽章”以公開鑰匙α_B解開得到”標單資訊

摘要值=m_1”，再將”標單資訊m_0”輸入(hash function 如 MD5)

得到另一個”標單資訊摘要值m_2”比較m_1和m_2是否相等,相等即

認證成功，表示簽章無誤。

例:

設投標金額 1000 萬元，以$\alpha_T=(n_T,e_T)=(24961,125)$加密

$C\equiv 1000^{125}\equiv 86 \pmod{24961}$

設標單資訊M_B=(ID, time, C)=(219 ,0617 ,86)

$x=M_B$，$k=100$，$m_B=f(x)=(m'_B,m''_B,m'''_B)=(19,17,86)$

簽章 $s_B \equiv m_B{}^{\beta_B} \pmod{n_B}$

$s'_B \equiv 19^{1709} \pmod{22969} \equiv 11036 \pmod{22969}$

$s''_B \equiv 17^{1709} \pmod{22969} \equiv 20011 \pmod{22969}$

$s'''_B \equiv 86^{1709} \pmod{22969} \equiv 10992 \pmod{22969}$

得到 (M_B, s_B) ， $M_B = (219,617,86)$

$s_B = (s'_B, s''_B, s'''_B) = (11036, 20011, 10992)$

(M_B, s_B) 以 $\alpha_A = (n_A, e_A) = (21311, 97)$ 加密傳送招標者 A，

$c_1 \equiv M'_B{}^{\alpha_A} \equiv 219^{97} \equiv 19709 \pmod{21311}$

$c_2 \equiv M''_B{}^{\alpha_A} \equiv 617^{97} \equiv 20980 \pmod{21311}$

$c_3 \equiv M'''_B{}^{\alpha_A} \equiv 86^{97} \equiv 6981 \pmod{21311}$

$c_4 \equiv s'_B{}^{\alpha_A} \equiv 11036^{97} \equiv 17313 \pmod{21311}$

$c_5 \equiv s''_B{}^{\alpha_A} \equiv 20011^{97} \equiv 20002 \pmod{21311}$

$c_6 \equiv s'''_B{}^{\alpha_A} \equiv 10992^{97} \equiv 289 \pmod{21311}$

招標者 A 以 $\beta_A = (n_A, d_A) = (21311, 433)$ 解密得到 (M_B, s_B)

$M'_B \equiv c_1{}^{\beta_A} \equiv 19709^{433} \equiv 219 \pmod{21311}$

$M''_B \equiv c_2{}^{\beta_A} \equiv 20980^{433} \equiv 617 \pmod{21311}$

$M'''_B \equiv c_3{}^{\beta_A} \equiv 6981^{433} \equiv 86 \pmod{21311}$

$s'_B \equiv c_4{}^{\beta_A} \equiv 17313^{433} \equiv 11036 \pmod{21311}$

$s''_B \equiv c_5{}^{\beta_A} \equiv 20002^{433} \equiv 20011 \pmod{21311}$

$s'''_B \equiv c_6{}^{\beta_A} \equiv 289^{433} \equiv 10992 \pmod{21311}$

解密得到 (M_B, s_B) ， $M_B = (219,617,86)$ ，

$$s_B = (s'_B, s''_B, s'''_B) = (11036, 20011, 10992)$$

把 M_B 輸入雜湊函數 $f(x)$ 得到

$$m_B = (m'_B, m''_B, m'''_B) = (19, 17, 86)$$

把 $s_B = (11036, 20011, 10992)$ 用 α_B 解密

$$\tilde{m}_B \equiv s_B{}^{\alpha_B} \pmod{n_B}$$

$$\Rightarrow \tilde{m}'_B \equiv 11036^{53} \pmod{22969} \equiv 19 \pmod{22969}$$

$$\tilde{m}''_B \equiv 20011^{53} \pmod{22969} \equiv 17 \pmod{22969}$$

$$\tilde{m}'''_B \equiv 10992^{53} \pmod{22969} \equiv 86 \pmod{22969}$$

$$\tilde{m}_B = (\tilde{m}'_B, \tilde{m}''_B, \tilde{m}'''_B) = (19, 17, 86)$$

驗證 m_B 和 $\tilde{m}_B$ 相等。

步驟(4)：招標商 A 回覆投標者 B，其投標成功，傳送回復資訊[競標項目 ID、投標時間 T、[*出價資訊*]$^{\alpha_T}$]。並將此回復資訊以私密鑰匙 β_A 做數位簽章，得到[*回覆資訊* $^{\beta_A}$] 並傳送給投標者 B，顯示其投標成功。

步驟(5)：等到結標日期，由 CA 公正機構傳送 β_T 給招標商 A，招標商 A 使用 β_T 將”標單資訊”中([*出價資訊*]$^{\alpha_T}$)，進行 RSA 解密。得到競標價錢，再將各個競標者的價錢進行比較，最高者得標，並公告得標資訊。

例:

把標單資訊中 $C=86$ 以 $\beta_T=(n_T,d_T)=(24961,197)$ 解密

求投標金額 $M \equiv 86^{197} \equiv 1000 \pmod{24961}$

故投標金額 1000 萬元。

密封競標再招標商 A 和投標者 B 之間傳遞訊息，傳遞時間可以用 RSA 法加上摘要值運算法來簡短運算，比原本單純使用 RSA 法運算更快，可以節省競標運算時間。

3.2 使用 ECC 在密封投標上

首由 CA 公正機構，發給招標商 A 一組公開鑰匙 α_A 和私密鑰匙 β_A，和一個 CA 認證的公開鑰匙 α_T，首先招標商 A 廣播”招標資訊”（競標項目、ID、開標時間 T、專屬此競標項目之公開鑰匙 α_T）。投標者 B 向 CA 註冊並獲得一組鑰匙，公開鑰匙 α_B 和私密鑰匙 β_B。

(1) 招標商 A 公告招標資訊並做招標資訊的數位簽章：

公告招標資訊為 m_A，對 m_A 做 ECC 數位簽章。

橢圓曲線 $E_P(a,b)$：$y^2 = x^3 + ax + b \pmod{p}$

在橢圓曲線 E 上取任一點 G_A

招標商 A 私密鑰匙 β_A

招標商 A 的公開鑰匙 $\alpha_A = \beta_A G_A$

選擇一亂數 r_A，並計算 $R_A = r_A G_A = (R_{Ax}, R_{Ay})$

計算簽署文 $s_A = r_A^{-1}(M_A - \beta_A R_{Ax})$

公告 $(m_A, (R_A, s_A))$，(R_A, s_A) 作為簽署文。

例:

橢圓曲線 $E_{23}(1,1)$：$y^2 = x^3 + x + 1 \pmod{23}$

取 $G = (11,20)$

設招標資訊 m_A=(ID, time, α_T)=$(m'_A, m''_A, m'''_A) = (500,100601,660)$

取私密鑰匙 $\beta_A = 5$

公開鑰匙 $\alpha_A = \beta_A G = 5(11,20) = (55,100)$

$r_A = 8$ ， $R_A = r_A G = 8(11,20) = (88,160)$

$s'_A = r_A^{-1}(m'_A - \beta_A R_{Ax}) = 3(500 - 440) = 180$

$s''_A = r_A^{-1}(m''_A - \beta_A R_{Ax}) = 3(100601 - 440) = 300483$

$s'''_A = r_A^{-1}(m'''_A - \beta_A R_{Ax}) = 3(660 - 440) = 660$

公告 $(m_A, (R_A, s_A))$

$m_A = (m'_A, m''_A, m'''_A) = (500,100601,660)$

$R_A = (R_{Ax}, R_{Ay}) = (88,160)$

$s_A = (s'_A, s''_A, s'''_A) = (180,300483,660)$

(2) 投標者 B 傳送標單資訊並做標單資訊的數位簽章：

標單資訊為 m_B，對 m_B 做 ECC 數位簽章。

標單資訊=［競標項目 ID、公開鑰匙 α_B、投標時間 T、

[*出價資訊的密文*]］。(首先對出價資訊做 ECC 加密法)

橢圓曲線 $E_P(a,b)$：$y^2 = x^3 + ax + b \pmod{p}$

在橢圓曲線 E 上取任一點 G_B

投標者 B 私密鑰匙 β_B

投標者 B 的公開鑰匙 $\alpha_B = \beta_B G_B$

選擇一亂數 r_B，並計算 $R_B = r_B G_B = (R_{Bx}, R_{By})$

計算簽署文 $s_B = r_B^{-1}(M_B - \beta_B R_{Bx})$

即得 $(m_B, (R_B, s_B))$，(R_B, s_B) 作為簽署文。

再將 (m_B, s_B) 以招標商 A 公開鑰匙 α_A 做 ECC 密碼加密，

$c_B = (c'_B, c''_B)$

$= (m_B, s_B) + ((r_B \alpha_A)_x, (r_B \alpha_A)_x)$

(c_B, R_B) 傳送給招標商 A。

招標商 A 對 (c_B, R_B)

$c_B = (c'_B, c''_B)$

$= (m_B, s_B) + ((r_B \alpha_A)_x, (r_B \alpha_A)_x)$

用私密鑰匙 β_A 解密，得到 $(m_B, (R_B, s_B))$ ，

再將 (R_B, s_B) 用來驗證。

驗證方法：$V_1 = R_{Bx} \alpha_B + s_B R_B$

$V_2 = m_B G_B$ ，檢驗 $V_1 \stackrel{?}{=} V_2$

若相等即驗證成功，此標單有效。

例:

橢圓曲線 $E_{23}(1,1)$ ： $y^2 = x^3 + x + 1 \pmod{23}$

取 $G = (11,20)$ ，設投標金額 M =200 萬元，$\alpha_T = (187, 340)$

$r_B = 7$ ， $R_B = r_B G = 7(11,20) = (77,140)$

$C = M + (r_B \alpha_T)_x = 200 + 7(187,340)_x = 1509$

設投標資訊m_B=(ID, time, C)=$(m'_B, m''_B, m'''_B) = (500,100610,1509)$

$\beta_B = 3$

$\alpha_B = \beta_B G = 3(11,20) = (33,60)$

$r_B = 7$ ， $r_B r_B^{-1} \equiv 1 \pmod{23}$ ，

$R_B = r_B G = (R_{Bx}, R_{By}) = 7(11,20) = (77,140)$

$s'_B = r_B^{-1}(m'_B - \beta_B R_{Bx}) = 10(500 - 231) = 2690$

$s''_B = r_B^{-1}(m''_B - \beta_B R_{Bx}) = 10(100610 - 231) = 1003790$

$s'''_B = r_B^{-1}(m'''_B - \beta_B R_{Bx}) = 10(1509 - 231) = 12780$

將(m_B, s_B) 以$\alpha_A = (55,100)$加密後傳送

$m_B = (m'_B, m''_B, m'''_B) = (500,100610,1509)$ ，

$s_B = (s'_B, s''_B, s'''_B) = (2690,1003790,12780)$

$R_B = (R_{Bx}, R_{By}) = (77,140)$

$c_1 = m'_B + (r_B \alpha_A)_x = 500 + 385 = 885$

$c_2 = m''_B + (r_B \alpha_A)_x = 100610 + 385 = 100995$

$c_3 = m'''_B + (r_B \alpha_A)_x = 1509 + 385 = 1894$

$c_4 = s'_B + (r_B \alpha_A)_x = 2690 + 385 = 3075$

$c_5 = s''_B + (r_B \alpha_A)_x = 1003790 + 385 = 1004175$

$c_6 = s'''_B + (r_B \alpha_A)_x = 12780 + 385 = 13165$

將(m_B, s_B) 以$\alpha_A = (55,100)$加密

得到 $c_B = (c'_B, c''_B)$

$= (m_B, s_B) + ((r_B \alpha_A)_x, (r_B \alpha_A)_x)$

$c'_B = (c_1, c_2, c_3) = (885, 100995, 1894)$

$c''_B = (c_4, c_5, c_6) = (3075, 1004175, 13165)$

$R_B = (R_{Bx}, R_{By}) = (77,140)$

傳送 $c_B = (c'_B, c''_B)$

$R_B = (R_{Bx}, R_{By}) = (77,140)$

將 $c_B = (c'_B, c''_B)$ 以 $\beta_A = 5$ 解密得到 $(m_B, s_B))$

$m'_B = c_1 - (\beta_A R_B)_x = 885 - (5(77,140))_x = 500$

$m''_B = c_2 - (\beta_A R_B)_x = 100995 - 385 = 100610$

$m'''_B = c_3 - (\beta_A R_B)_x = 1894 - 385 = 1509$

$s'_B = c_4 - (\beta_A R_B)_x = 3075 - 385 = 2690$

$s''_B = c_5 - (\beta_A R_B)_x = 1004175 - 385 = 1003790$

$s'''_B = c_6 - (\beta_A R_B)_x = 13165 - 385 = 12780$

得到 $(m_B, (R_B, s_B))$

$m_B = (m'_B, m''_B, m'''_B) = (500, 100610, 1509)$

$R_B = (R_{Bx}, R_{By}) = (77,140)$

$s_B = (s'_B, s''_B, s'''_B) = (2690, 1003790, 12780)$

驗證方法：

$V_1 = R_{Bx}\alpha_B + s_B R_B \pmod{23}$

$V_2 = m_B G \pmod{23}$

$V_1 = (V_1', V_1'', V_1''')$ ，$V_2 = (V_2', V_2'', V_2''')$

$V_1' = 77(33,60) + 2690(77,140) = (3,18) \pmod{23}$

$V_2' = m_B' G = 500(11,20) = (3,18) \pmod{23}$

$V_1'' = 77(33,60) + 1003790(77,140) = (19,22) \pmod{23}$

$V_2'' = m_B'' G = 100610(11,20) = (19,22) \pmod{23}$

$V_1''' = 77(33,60) + 12780(77,140) = (16,4) \pmod{23}$

$V_2''' = m_B''' G = 1509(11,20) = (16,4) \pmod{23}$

，檢驗 $V_1 \stackrel{?}{=} V_2 \Rightarrow V_1 = V_2$

(3) 招標商 A 回覆投標者 B，其投標成功，傳送回復資訊[競標項目 ID、投標時間 T、[*出價資訊的密文*]]。並將此回復資訊以私密鑰匙 β_A 做 ECC 簽章，得到[*回覆資訊的簽署文*]並傳送給投標者 B，顯示其投標成功。

例:

橢圓曲線 $E_{23}(1,1)$ ： $y^2 = x^3 + x + 1 \pmod{23}$

取 $G = (11,20)$

設回復資訊 m_C=(ID, time , C)=$(m'_C, m''_C, m'''_C) = (500,100610,1509)$

取私密鑰匙 $\beta_A = 5$

公開鑰匙 $\alpha_A = \beta_A G = 5(11,20) = (55,100)$

$r_A = 8$ ， $R_A = r_A G = 8(11,20) = (88,160)$

$s'_C = r_A^{-1}(m'_C - \beta_A R_{Ax}) = 3(500 - 440) = 180$

$s''_C = r_A^{-1}(m''_C - \beta_A R_{Ax}) = 3(100610 - 440) = 300510$

$s'''_C = r_A^{-1}(m'''_C - \beta_A R_{Ax}) = 3(1509 - 440) = 3207$

回覆 $(m_C, (R_A, s_C))$

$m_C = (m'_C, m''_C, m'''_C) = (500,100610,1509)$ ， $R_A = (88,160)$

$s_C = (s'_C, s''_C, s'''_C) = (180,300510,3207)$

(4) 等到結標日期，由 CA 公正機構傳送 β_T 給招標商 A，招標商 A 使用 β_T 將”標單資訊”中([*出價資訊的密文*])，進行 ECC 解密。

得到競標價錢，再將各個競標者的價錢進行比較，最高者得標，並公告得標資訊。

例：

加密投標金額 C=1509 萬元， $\beta_T = 17$

$R_B = r_B G = 7(11,20) = (77,140)$

$M = C - (\beta_T R_B)_x = 1509 - 17 \times 77 = 200$

故投標金額 200 萬元

3.3 RSA 及 ECC 在密封標單之比較

本篇論文以RSA公開鑰匙密碼系統和橢圓曲線密碼系統，對電子競標中的密封投標做其應用。在密碼系統中，RSA密碼系統的優點有原理簡單易於使用，容易了解。但隨著電腦的發達，計算速度越來越快，RSA密碼系統的安全性，越來越容易被破解。因此需要增加RSA的安全性，提高鑰匙的位數，一般提高到1024位元以上的長度才有足夠安全性。但是，鑰匙長度增加使得解密速度大大降低，尤其是使用RSA系統的電子商務，帶來很大的負擔。因為RSA密碼系統，在運算上需要用到大指數的算法，因此在運算上需要較長的時間，也浪費較多的資源。

在相同的安全強度下，ECC的鑰匙長度與RSA的鑰匙長度比較如下表(1)所示。

安全性 / 演算法	2^{80}	2^{112}	2^{128}	2^{192}	2^{256}
RSA長度(位元)	1024	2048	3072	7680	15360
ECC長度(位元)	161	224	256	384	512
金鑰長度比	6:1	9:1	12:1	20:1	30:1

如上表(1)ECC的鑰匙長度或數位簽章的長度遠比RSA小。所以無論演算方式為何，從速度或節省空間的角度， ECC都是優於RSA。ECC密碼系統只需採用較小的鑰匙就可以達到和RSA密碼系統相同的安全度，因為使用了離散對數的方法，因此比RSA密碼系統來說，在同樣安全度下，所需的鑰匙較小。

加上電腦硬體的限制，CPU獲的RAM的限制，若要處理多筆運算，使用運算量小卻能提供一樣安全性的密碼系統，ECC就有明顯優勢。相信ECC在未來會有更多廣泛的應用。

參考文獻

[1]張真誠/林祝興：資訊安全技術與應用，全華科技圖書股份有限公司，2006 年

[2]賴溪松/韓亮/張真誠：近代密碼學及其應用，旗標出版社，2004 年

[3]張博竣：資訊安全管理實務，文魁資訊股份有限公司，2004 年

[4]沈淵源：密碼學之旅與 MATHEMATICA 同行，全華科技圖書股份有限公司，2006 年

[5]賴溪松/蔡育斌:資訊安全入門,全華科技圖書股份有限公司,2004 年

[6]黃明祥：網路安全與密碼學， 2007 年

[7]陳彥學：資訊安全理論與實務，文魁資訊股份有限公司，2000 年

[8]戴江淮：網路安全，全威圖數有限公司，2007 年

[9]黃明祥：資訊與網路安全慨論，2005 年

[10]戴元軍；安全的電子拍賣方案，2003 年

[11]蕭勝文：電子競標系統之研究，中央大學資訊工程研究所碩士論文，2004 年

[12]胡國新:設計植基於自我驗證公開鑰匙系統之安全線上電子拍賣機制，大葉大學，資訊管理研究所， 2000 年

[13]林志堯：電子競標之異議處理系統的研究設計，長庚大學電機工程研究所，2003 年

[14]張薰伊：橢圓曲線電子現金，東海大學數研所碩士班，2009 年

[15]C.C. Chang and Y.P. Lai S：”A Flexible Data Attachment Scheme on E-Cash”，2003

[16] C.C. Chang and Y.F. Chang：” Efficient Anonymous Auction Protocols with Freewheeling Bids”，2003

附 錄

Abstract

In recent years, the demand for information and electronic services is growing. Already the exchange of sensitive information, such as credit card numbers and bank transactions, over the Internet is common practice. Protecting data and electronic systems is crucial to our way of life.

The paper is divided into three chapters. The first chapter describes the development of the cryptographic system in the daily life, and the application of the e-commerce such as electronic cash, e-bidding. The second chapter gives the basic knowledge on cryptography such as RSA Algorithm, elliptic curve and the hash function, we also introduce electronic bid for two categories: public bid and sealed bid. Finally, we apply the RSA and elliptic curve cryptography to the sealed bid, and also study the differences between these two methods in the last chapter.